

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Frederick Johannes Bruwer

Application No.: 10/014,664

Group No.: 2131

Filed: 12/14/2001

Examiner: A. Moorthy

For: METHOD AND APPARATUS FOR TRANSFERRING DATA

**Mail Stop Appeal Briefs – Patents**

**Commissioner for Patents**

**P.O. Box 1450**

**Alexandria, VA 22313-1450**

**TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 41.37)**

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on September 4, 2007.

2. STATUS OF APPLICANT

This application is on behalf of a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

small entity	\$255.00
--------------	----------

<b>Appeal Brief fee due</b>	<b>\$255.00</b>
-----------------------------	-----------------

**4. EXTENSION OF TERM**

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for three months:

Fee:	\$525.00
------	----------

If an additional extension of time is required, please consider this a petition therefor.

**5. TOTAL FEE DUE**

The total fee due is:

Appeal brief fee	\$255.00
Extension fee (if any)	\$525.00

<b>TOTAL FEE DUE</b>	<b>\$780.00</b>
----------------------	-----------------

**6. FEE PAYMENT**

Payment will be made by credit card upon e-filing of this paper.

**7. FEE DEFICIENCY**

If any additional extension and/or fee is required, charge Deposit Account No. 10-1213.

Date: February 1, 2008

Reg. No.: 30548  
Tel. No.: 703-415-1500  
Customer No.: 23294

\_\_\_\_\_  
/wab/  
Signature of Practitioner  
William A. Blake  
Jones, Tullar & Cooper, PC  
PO Box 2266 Eads Station  
Arlington, VA 22202

**Practitioner's Docket No. P.19385 *PATENT***

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Frederick Johannes Bruwer  
Application No.: 10/014,664 Group No.: 2131  
Filed: December 14, 2001 Examiner: A. Moorthy  
For: METHOD AND APPARATUS FOR TRANSFERRING DATA

**Commissioner for Patents  
Washington, D.C. 20231**

**ATTENTION: Board of Patent Appeals and Interferences**

**APPEAL BRIEF  
(37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on September 4, 2007.

The fees required under § 41.20, and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

The following sections are included as required by 37 C.F.R. 41.37(c) (1):

<u>SECTION</u>	<u>PAGE</u>
I. REAL PARTIES IN INTEREST	2
II. RELATED APPEALS AND INTERFERENCES	3
III. STATUS OF CLAIMS	4
IV. STATUS OF AMENDMENTS	5
V. SUMMARY OF CLAIMED SUBJECT MATTER	6
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	11
VII. ARGUMENT	12
VIII. CLAIMS APPENDIX	30
IX. EVIDENCE APPENDIX	40
X. RELATED PROCEEDINGS APPENDIX	41

**I REAL PARTIES IN INTEREST**  
(37 C.F.R. § 41.37(c) (1) (i))

The real party in interest in this appeal is the assignee of record of the subject application,  
AZOTEQ (PTY) LTD of Paarl, South Africa.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL  
(34 C.F.R. § 41.37(c) (1) (vi))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

**III. STATUS OF CLAIMS**  
(37 C.F.R. § 41.37(c) (1) (iii))

**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

The number of claims in the application is 63.

**B. STATUS OF ALL OF THE CLAIMS IN APPLICATION**

1. Claims canceled: 1-24, 38
2. Claims withdrawn from consideration but not canceled: none
3. Claims objected to: none
4. Claims allowed or confirmed: none
5. Claims rejected: 25-37; 39-63

**C. CLAIMS ON APPEAL**

The claims on appeal are: 25-37; 39-63. See Appendix in Section VIII for listing.

**IV. STATUS OF AMENDMENTS**  
(37 C.F.R. § 41.37(c) (1) (iv))

No Amendments have been filed since the final Office Action was mailed.

**V SUMMARY OF CLAIMED SUBJECT MATTER**  
(37 C.F.R. § 41.37(c) (1) (v))

The invention recited in independent claims 25 and 52 relates to a method and apparatus, respectively, for securely transferring data between a transmitter and a receiver. Typical applications of the invention include wireless remote controllers for garage door openers, door locks, remote keyless entry systems, gate controllers etc. It is normally a requirement in these security related applications that only authorized remote controllers are able to communicate with the receiver that controls actuation of a device and transfers commands. The subject invention specifically relates to a method and apparatus for insuring that only authorized remote transmitter encoders can transfer commands to a receiver decoder.

The invention represents an improvement on a known technique disclosed in Yoshizawa, EP 0311112 A2, which is of record in the subject application. In Yoshizawa's system, clocks or timers in a transmitter and a receiver are first synchronized with one another by being simultaneously reset to a common initial value e.g. zero. The value of the transmitter timer is then sent to the receiver each time the transmitter communicates with the receiver. The receiver compares its timer value with the received transmitter timer value. If the two values match, then this confirms that the transmission is from an authorized transmitter. If the values do not match, then the transmission is not from an authorized transmitter and the receiver will not permit actuation of the controlled device.

The present invention avoids the need for resetting the transmitter and receiver timers for normal operation, which is a notable drawback of Yoshizawa's system if multiple remote control transmitters are employed as is a typical requirement for applications such as door locks, vehicle remote keyless entry (RKE) systems and garage door controllers. As noted before, during the synchronization step in Yoshizawa, the transmitter and receiver timers must be reset at the same



**V SUMMARY OF CLAIMED SUBJECT MATTER**  
(37 C.F.R. § 41.37(c) (1) (v))

instant. This makes it totally impractical, if not near impossible, to use more than one transmitter with a single receiver because all of these devices would have to be reset at the same instant.

The subject claimed invention overcomes the aforementioned drawback of the Yoshizawa system by providing a system that does not require reset of the system device timers for synchronization. Instead, the invention recited in independent claims 25 and 52 employs what is referred to as a Timer Relationship Value (TRV) which is generated from the mathematical difference between the values of the transmitter and receiver timers and is independently calculated for each transmitter in the system.

Referencing the Description of Preferred Embodiment section at paragraph [0066] on page 14, an encoder 10 is shown in Figure 1 which forms part of a transmitter. The encoder 10 includes a continuously running timer 22, from which is derived, a timer information portion 30 of a dataword 28 as discussed in paragraph [0072] on page 15 and illustrated in Figure 5. Figure 6 illustrates a transmission word 70 which includes, among other values, an encrypted version 74 of the data word 28 as discussed in paragraph [0080] on page 16. The transmission word 70 is transmitted to a receiver decoder 80 as illustrated in Figure 3, at which the word is decrypted. As discussed in paragraph [0083], the decoder 80 includes a decoder timer 86.

A learning process is discussed beginning on page 19 in paragraph [0085]. As discussed in the specification in paragraphs [0088] and [0089] on page 20, the TRV (referred to as Tr value in the spec) is generated during the learning process. During this process, the decoder 80 receives identification information from the transmitter encoder 10, including the value of the encoder timer 22 and determines the difference between the encoder timer value and the decoder timer value at that instant. For example, if the transmitter encoder timer value is “120” and the

**V SUMMARY OF CLAIMED SUBJECT MATTER**  
(37 C.F.R. § 41.37(c) (1) (v))

receiver decoder timer value is “1243, then the TRV would be  $1243-120=1123$ . The TRV is stored in the decoder 80 and is then used each time a data transmission (e.g. command) is received from the transmitter encoder. During operation, the difference between the encoder and decoder timer values is calculated and then compared to the TRV stored in the decoder 80. If the difference is within a certain amount of the stored TRV, this then confirms that the received signal is from the transmitter encoder that was authorized during the learning process and the command will be executed. However, if it differs more than the certain amount, then the command is assumed to be from an unauthorized transmitter and will not be executed.

The foregoing receiver decoder operation, wherein the TRV of the incoming transmission word from the encoder is analyzed to verify the authenticity of the transmitter encoder, is illustrated in Figure 11 and discussed in paragraphs [00140]-[00143] on pages 31-32.

Method claim 25 thus recites a method of securely transferring data from an encoder to a decoder, wherein the encoder includes an encoder timer and the decoder includes a decoder timer. The method carries out the steps discussed above wherein during a learning process, the value of the encoder timer is received at the decoder which determines a mathematical difference value between the values of the encoder and decoder timers. This difference is stored as a timer relationship value in the decoder. Now, during normal operation, a data word is encrypted at the encoder to form a transmission word, the data word including information identifying a present value of the encoder timer. The transmission word is transmitted to the decoder, which decrypts the transmission word and determines the mathematical difference value between the present encoder and decoder timer values. Finally, the transmission word is validated by comparing the

**V SUMMARY OF CLAIMED SUBJECT MATTER**  
(37 C.F.R. § 41.37(c) (1) (v))

mathematical difference value between the present encoder and decoder timer values with the timer relationship value stored in said decoder.

Claim 52 is essentially an apparatus version of claim 25 and discloses an apparatus for transferring data which includes the encoder and decoder recited in claim 25, wherein the decoder includes a decoder timer, a receiver unit for receiving the encrypted transmission word, a decryption unit for decrypting the received transmission word to extract, at least, the timer information from the encoder, a difference determination unit for determining the mathematical difference value between the encoder and decoder timer values, and a comparator unit for comparing the mathematical difference value and the timer relationship value stored in the decoder, to determine the validity of the transmission word. As in claim 25, claim 52 specifies that the timer relationship value is established during a learning process of the encoder and decoder and is representative of the mathematical difference between the value of the encoder timer that is received by the decoder during the learning process and the value of the decoder timer during the learning process.

Dependent claim 60 is the only claim on appeal that employs means plus function language pursuant to 35 U.S.C. 112, paragraph six. This claim is actually similar in scope to claim 52. The claim recites a decoder for use in the method of claim 25 which includes a timer, an input to receive the transmission word, a decryption unit to decrypt the transmission word and obtain the transmitted timer information, memory to store the timer relationship value and a comparison unit to compare the transmitted timer information to time information generated by the decoder timer and to the stored timer relationship value, and means, responsive to the comparison unit, to activate an output if certain criteria are met in the comparison. The

**V SUMMARY OF CLAIMED SUBJECT MATTER**  
(37 C.F.R. § 41.37(c) (1) (v))

comparison unit and the last, means plus function element are actually carried out by software modules in the decoder 80 as discussed in paragraphs [00139]-[00143] on pages 31 and 32 of the specification and illustrated in Figure 11.

**VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**  
(37 C.F.R. § 41.37(c) (1) (vi))

1. Whether claims 25-30, 34-37 and 39-60 are anticipated under 35 U.S.C. 102(b) by Farris et al., Jr., U.S. Patent No. 6,154,544.

2. Whether claim 31 is unpatentable under 35 U.S.C. 103(a) over Farris et al, Jr. U.S. Patent No. 6,154,544 in view of Belt et al., U.S. Patent No. 5,446,904.

3. Whether claims 32, 33 and 61-63 are unpatentable under 35 U.S.C. 103(a) over Farris et al, Jr. U.S. Patent No. 6,154,544 in view of Rysko et al., U.S. Patent No. 5,155,729.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

1. REJECTION OF CLAIMS 25-30; 34-37 AND 39-60 UNDER 35 U.S.C. 102

Introduction

At the outset, it is fundamental that in order for a reference to anticipate a claim under 35 U.S.C. 102, the reference must disclose each and every element recited in the claim. Further, while MPEP Section 2111 sets forth that claims must be given their broadest reasonable interpretation, it is also well established that this interpretation must be consistent with the specification.

As will be established herein, the rejections of claims 25-30; 34-37 and 39-60 over Farris et al. are completely without merit. In all candor, Applicant is frankly baffled by the Examiner's assertion that each and every element of the rejected claims is anticipated by Farris et al., even when the broadest possible interpretation of the claims consistent with the specification is applied.

Claims 25, 28, 30, 35, 36, 37, 44, 46, 48, 49, 52, 54, 55 and 59

In Section 7 of the final Office Action mailed May 1, 2007, the Examiner asserts that each element of independent claims 25 and 52 is disclosed in Farris et al. at column 3, line 1 through column 4, line 34, which is effectively the entire Summary of the Invention section of Farris et al. The lack of a more specific citation in this large excerpt from Farris et al for each of the claim elements is telling in and of itself of what appears to be a failure by the Examiner to comprehend the detailed elements of the claims and their recited relationship to one another.

For the convenience of the Board, the cited excerpt from Farris et al. is reproduced below from the online full text version of the patent. As can be readily discerned from this excerpt, the Farris et al. system does not use a timer based code scheme at all. Not surprisingly then, only

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

two of the seven lettered elements of claim 25 are actually disclosed in Farris et al. as will be discussed further below:

“The invention relates in general to an electronic system for providing remote security for entry or actuation of a particular device. Such a system may include a transmitter and receiver set, for instance with a hand-held transmitter and a receiver associated with a vehicle such as an automobile or the like. The transmitter, upon signaling the receiver, causing the vehicle to start up or to perform other functions. The system may also be useful in a barrier operator system such as a garage door operator by allowing the garage door to be opened and closed in a relatively secure fashion while preventing persons who may be intercepting the radio frequency signals from being able to, although unauthorized, cause the vehicle to begin running or to allow access to the garage.

The system includes a transmitter generally having means for developing a fixed code and a rolling or variable code. **The rolling or variable code is changed with each actuation of the transmitter.** The fixed code remains the same for each actuation of the transmitter. In the present system, the transmitter includes means for producing a 32-bit frame comprising the fixed portion of the code and a second 32-bit frame comprising the variable portion of the code. The 32-bit rolling code is then mirrored to provide a 32-bit mirrored rolling code. The 32-bit mirrored rolling code then has its most significant bit "deleted" by setting it to zero. The transmitter then converts the 32-bit fixed code and the mirrored variable code to a three-valued or trinary bit fixed code and a three-valued or trinary bit variable code or rolling code.

To provide further security, the fixed code and the rolling codes are shuffled so that alternating trinary bits are comprised of a fixed code bit and a rolling code bit to yield a total of 40 trinary bits. The 40 trinary bits are then packaged in a first 20-trinary bit frame and a second 20-trinary bit frame which have proceeding them a single synchronization and/or identification pulse indicating the start of the frame and whether it is the first frame or the second frame. Immediately following each of the frames, the transmitter is placed into a quieting condition to maintain the average power of the transmitter over a typical 100 millisecond interval within legal limits promulgated by the United States Federal Communications Commission. The first trinary frame and the second trinary frame are used to modulate a radio frequency carrier, in this case via amplitude modulation to produce an amplitude modulated encrypted signal. In a preferred embodiment, the radio frequency signal is amplitude modulated. The amplitude modulated signal is then launched and may be received by an AM receiver. In the preferred embodiment, the AM receiver receives the amplitude modulated signal, demodulates it to produce a pair of trinary bit encoded frames.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

The trinary bits in each of the frames are converted on the fly to 2-bit or half nibbles indicative of the values of the trinary bits which are ultimately used to form two 16-bit fixed code words and two 16-bit variable code words. The two 16-bit fixed code words are used as a pointer to identify the location of a previously stored rolling code value within the receiver. The two 16-bit rolling code words are concatenated by taking the 16-bit word having the more significant bits, multiplying it by 310 and then adding it to the second of the words to produce a 32-bit encrypted rolling code. In order to make certain that if the transmitter was inadvertently actuated a number of times, the authorized user can still start his car or gain entry to his garage. **The 32-bit encrypted code is then compared via a binary subtraction with the stored rolling code. If the 32-bit code is within a window or fixed count, in the present embodiment 1000, the microprocessor produces an authorization signal which is then responded to by other portions of the circuit to cause the garage door to open or close as commanded.** In the event that the code is greater than the stored rolling code, plus 1000, indicative of a relatively large number of incrementations, the user is not locked out of the garage, but is allowed to provide further signals or indicia to the receiver that he is an authorized user without any significant degradation of the security. This is done by the receiver entering an alternate mode requiring two or more successive valid codes to be received, rather than just one. If the two or more successive valid codes are received, the garage door will open. However, in order to prevent a person who has previously or recently recorded a recent valid code from being able to obtain access to the garage, a trailing window, in this case starting at a count of 300 less than the present stored count and including all code values between the present stored count and 300 less is compared to the received code. If the received code is within this backward window, the response of the system simply is to take no further action, nor to provide authorization during that code cycle on the assumption that the code has been purloined.

Thus, the present system provides important advantages over the previous garage door operator systems and even previous rolling code systems. The system provides a multiple segmented windowed system which provides a valid code window, a second relatively insecure code window in which two successive valid codes must be received and finally a window in which no valid codes are recognized due to the likelihood of the receiver having been stolen.

It is a principal object of the present invention to provide a security system involving a radio frequency transmitter and receiver wherein multiple security conditions may exist requiring different levels of signal security.



**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

It is another object of the present invention to provide a secure radio transmitter receiver system which may rapidly and easily decode a relatively large code combination.” (Emphasis Added)

As the bolded sentences in the above excerpt clearly indicate, the Farris et al. system is based on a known technique referred to as “rolling code” in which each time the remote transmitter is actuated by a user, e.g. to open a garage door, a rolling code generated by the transmitter is incremented. This rolling code is then sent to the receiver which compares the rolling code to a previously stored rolling code in the receiver to determine the authenticity of the transmission from the transmitter. The Farris et al. system is obviously more involved than a standard rolling code technique, but for the purpose of the rejection, it is sufficient to note that the Farris et al. system, is clearly is not a timer based system in which continuously changing timer values are compared. As a result, Farris et al. cannot possibly anticipate either of the independent claims 25 and 52.

With specific reference to claim 25, Farris et al. do not disclose any of the bolded elements in the following copy of the claim:

25. A method of securely transferring data from an encoder to a decoder,  
**said encoder including an encoder timer and said decoder including a**  
**decoder timer**, said method including the steps of:
- (a) **during a learning process receiving a value of said encoder**  
**timer at said decoder and determining a mathematical difference value**  
**between said value of said encoder timer and a value of said decoder timer;**
  - (b) **storing said mathematical difference value as a timer**

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

**relationship value in said decoder;**

**(c) at the encoder encrypting a data word to form a transmission word, said data word including information identifying a present value of said encoder timer;**

**(d) transmitting the transmission word to the decoder;**

**(e) at the decoder decrypting the transmission word; and**

**(f) determining a mathematical difference value between said present encoder timer value and a present decoder timer value; and**

**g) validating the transmission word by comparing the mathematical difference value between said present encoder timer value and said present decoder timer value with said timer relationship value stored in said decoder.**

The deficiencies of the rejections over Farris et al. are so extensive that Applicant cannot understand why the Examiner insists on maintaining the rejection. In the Examiner's Response to Arguments set forth in Section 6 of the final Office Action dated May 1, 2007, the Examiner does not even address the specific arguments made by the Applicant in the Amendment filed January 22, 2007 regarding the failure of Farris et al. to disclose the elements of any of the rejected claims. Instead, the Examiner completely ignores the language of the claims and takes issue with Applicant's assertion that the codes in Farris have nothing to do with timer values. The Examiner notes this one assertion and cites a completely different section of Farris et al. as supporting the assertion that the codes employed in Farris et al. are timer based. The additional

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

excerpt reproduced below is completely irrelevant to the issue of the type of codes employed in Farris et al. or the method used for transmitter authentication. As such, the passage clearly fails to provide any support for the assertion that Farris et al. discloses the invention recited in claims 25 and 52:

“6. Applicant's arguments filed 22 January 2007 have been fully considered but they are not persuasive.

On page 13, the applicant argues that the codes employed in the Farris system have nothing to do with timer values.

The examiner respectfully disagrees. The examiner refers the applicant to FIGS. 8A through 8F and, in particular, to FIG. 8A, the operation of the receiver is set forth therein. In a step 700, an interrupt is detected and acted upon from the radio input pin. The time difference between the last edge is determined and the radio inactive timer is cleared in step 702. A determination is made as to whether this is an active time or inactive time in a step 704, i.e., whether the signal is being sent with carrier or not. If it is an inactive time, indicating the absence of carrier, control is transferred to a step 706 to store the inactive time in the memory and the routine is exited in a step 708. In the event that it is an active time, the active time is stored in memory in a step 710 and the bit center is tested in a step 712. If the bit counter zero, control is transferred to a step 714, as may best be seen in FIG. 8B and a test is made to determine whether the inactive time is between 20 milliseconds and 55 milliseconds. If it is not, the bit counter is cleared as well as the rolling code register and the fixed code register in step 716 and the routine is exited in step 718.”

The foregoing passage has nothing to do with whether the codes that are employed in the Farris et al. system vary in accordance with a timer. Figs. 8A through to 8F to which the examiner refers are clearly designated (col. 7, lines 57, 58) as describing operation of the receiver. The timing at the receiver referred to by the examiner concerns the synchronization of the receiver decoder to correctly identify the transmitted stream of data. This is standard practice in the reception of data, but bears no resemblance to the timer based codes as employed in the

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

claimed subject invention. More importantly, the foregoing passage provides no support for the contention that Farris et al. discloses the method of claim 25 or the corresponding apparatus of claim 52.

As already discussed, the claimed subject invention employs timers in the receiver decoder and in each transmitter encoder, whose values are compared to one another during learning and normal operation of the system. During subsequent operation of the system, the mathematical difference between the two values of the encoder and the decoder timers is compared to the stored timer relationship value to authenticate the encoder transmission. In this manner, the encoder and decoder timers need not be synchronized with one another during start up of the system.

In view of the foregoing, Farris et al. clearly fails to anticipate either method claim 25 or corresponding apparatus claim 52. Farris et al. disclose no encoder or decoder timer that will influence the data word to be encrypted or decrypted, no TRV, nor calculating a difference and storing a value related to the difference between an encoder and decoder timer during learn mode.

In view of the foregoing, the rejection of independent claims 25 and 52, as well as the rejection of each of the dependent claims are clearly in error and should be REVERSED.

In addition, a number of the dependent claims recite additional features that are also not disclosed in Farris et al., thus providing additional reasons why these claims are not anticipated by Farris et al. A discussion of these claims follows.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

Claims 26, 27

Claim 26 is dependent on claim 25 and recites that the timer relationship value (TRV) in the decoder is updated upon receipt of a valid transmission word to remove any discrepancies in the relationship between the encoder timer, decoder timer and the timer relationship value, without affecting the decoder timer. Claim 27 is dependent on claim 26 and recites that this updating is only done when necessary.

Farris et al. does not disclose a TRV in the decoder or an equivalent. In Farris et al. the stored counter value is updated when a new valid code is received. The section referred to by the examiner (col. 8, line 57 to col. 9, line 26) does not mention a timer. It does mention the comparison with the “last code received.” Clearly this code does not change with time as it is still the “last code received.” Thus, for these additional reasons, claims 26 and 27 are not anticipated by Farris et al.

Claim 29

Claim 29 is dependent on claim 28 and specifies that the user derived information is variable via one or more inputs to the encoder and is not known to a manufacturer of the encoder. The concept of user derived information that is not known to the manufacturer (for security purposes) is a very specific, clear concept. Once again, however, the Examiner cites a paragraph in Farris et al., col. 7, lines 1 – 26, which makes no mention of and has absolutely nothing to do with this concept. Thus, claim 29 is patentable over Farris et al. for this reason also.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

Claim 34

Claim 34 is dependent on claim 25 and further specifies the step of forming a plurality of transmission words, each transmission word being different from the other transmission words and being based at least on respective encoder high speed timer information, in response to a single activation of the encoder. In contrast, Farris et al. disclose a system whereby a code word is constructed and repeatedly transmitted while the transmitter is activated. No mention is made of the operation changing. According to Farris et al., once the button is released and then operated again, the code word will change and will again be continuously transmitted (repeated) in a sequence until the transmission is halted.

The claimed invention employs a high speed timer to vary the code words that are transmitted during a single transmitter activation (for an extended period of time) that may stretch over several code words. This is an action of the transmitter encoder. The section in Farris et al. referred to by the Examiner (col. 8, lines 26 – 56) relates to the receiver. Once again, Farris et al. does not even remotely disclose the limitations of claim 34. Thus, for this reason also, claim 34 is patentable over Farris et al.

Claim 39

Claim 39 is dependent on claim 25 and recites that multiple encoders are used with a single decoder comprising a single timer and multiple timer relationship values and wherein the various timer relationship values are determined, one for each encoder during its respective learning process.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

Once again, Farris et al. do not disclose the concept of a timer relationship value. Thus, Farris et al. cannot disclose the specific concept of employing multiple timer relationship values, one for each encoder.

Claim 40

Claim 40 is also dependent on claim 25 and specifies the step of ensuring that the encoder timer at its slowest variance is faster than the decoder timer at its fastest variance. Farris does not have chronological time derived code words as has already been discussed. Not surprisingly then, Farris et al. cannot and do not disclose the specific concept of ensuring that the encoder timer is faster than the decoder timer.

Claim 41

Claim 41 is dependent on claim 39 and recites that if the decoder timer lies within a predetermined window when a valid transmission word is received, the decoder timer is re-synchronised with the encoder timer by automatically adjusting the timer relationship value to remove any discrepancies in the relationship between the timers and the timer relationship value.

In Farris et al., re-synchronization is achieved by replacing the stored counter value with the latest decoded counter received from the encoder (see col. 9, line 19). In the present invention the decoder has a timer that runs independent from the encoder timer. Just as any conventional timers, the decoder and encoder timers will experience a drift against each other over a period of time. This may be days, months or years depending on the quality of implementation. To re-synchronize, the decoder timer is not affected since this would affect other transmitters working with the same receiver, (and they have different drift) but the timer relationship value of the particular encoder/decoder path is adjusted.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

As already noted, Farris et al. do not anticipate claim 25 and 39. In addition, nowhere in Farris et al. is disclosed the foregoing concept of re-synchronizing the encoder timer in the manner recited in claim 41. Thus, for this reason also, claim 41 is patentable over Farris et al.

Claim 42

Claim 42 adds even more specific elements that are nowhere disclosed in Farris et al. In claim 42, it is specified that the re-synchronization recited in claim 41 is effected by a bi-directional transfer of data between the encoder and decoder. There is no mention in Farris et al. of a decoder/receiver unit communicating information to an encoder/transmitter unit in the foregoing manner.

Claim 43

Claim 43 recites the method of claim 25 wherein the timer relationship value or a window is adjusted in size to compensate for drift between the encoder timer and the decoder timer, before validation occurs, such adjustment being based at least on the time period elapsed since the last adjustment of the timer relationship value.

The system disclosed by Farris et al. has no means to determine a time period between a previously received code word and a next code word. There is absolutely no mention of this concept in Farris et al. and, in fact, it would have no meaning in Farris et al. since the code words are incremented with operations, thus the concept of drift over time (days or months) has no meaning in Farris.

Claim 45

Claim 45 recites the method of claim 25 wherein a window size is assigned to the decoder and the encoder timer is operated to ensure that the encoder timer information does not



**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

fall outside the window for a valid transmission of a transmission word in normal operational circumstances.

Once again, Farris et al. discloses no encoder timer and, as such, has no control over such encoder timer operation.

Claim 47

Claim 47 is dependent on claim 46, which is dependent on claim 25. Claim 47 is similar to claim 43 and specifies that the window size is dynamically adjusted and such adjustment is based on the time period elapsed since the previous adjustment of the timer relationship value. The same comments made with respect to claim 43 apply to claim 47. Farris et al. is completely devoid of any teaching of the elements of claim 47.

Claim 50

Claim 50 is dependent on claim 25 and recites that the transmission data word also includes a timer value that changes fast so that each transmission word in a sequence of transmission words which are transmitted based on a single continuous activation of the encoder, differs from the other transmission words. Once again, this specific, clear concept is nowhere found in Farris et al.

Claim 51

Claim 51 is dependent on claim 25 and specifies that a higher security re-synchronization of the encoder and decoder timers is achieved at least by using the decoder to generate control signals that are used to, directly or indirectly, control the activation of the encoder. As mentioned before, Farris does not disclose bi-directional communication and, as such, cannot anticipate the decoder generating signals to affect the encoder.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

Claim 54

Claim 54 discloses the apparatus of claim 52 wherein the timer relationship value is adjusted before checking the validity of a received transmission word, such adjustment being based at least on a known drift between the encoder timer and the decoder timer as well as the time elapsed since a previous adjustment of the timer relationship value.

There is no disclosure in Farris et al. of adjusting any information of the decoder before using it to make a comparison when a valid transmission is received.

Claim 56

Claim 56 recites the apparatus of claim 55 wherein the window size is adjusted before checking the validity of a received transmission word, said adjustment being based at least on the time period elapsed since the reception of a previously received valid transmission word.

Farris et al. do not disclose measuring the time since a previous reception of a valid transmission.

Claim 57

Claim 57 is dependent on claim 52 and further specifies that a re-synchronization of the encoder and decoder can be achieved by the decoder providing control signals for the encoder inputs. Once again, nowhere in Farris et al. is this specific concept disclosed. Farris et al. do not disclose communication from a decoder to exert any control or transfer information to an encoder.

Claim 58

Claim 58 is dependent on claim 25 and specifies that the method uses a transmitter which includes an encoder timer and an encryption unit for encrypting data which at least in part is

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

based on timer information from the encoder timer thereby to form the transmission word, and wherein the encoder timer is permitted to run only for a limited period after each activation of the transmitter. Once again, there is no disclosure in Farris et al. of this specific concept.

Claim 60

Claim 60 is dependent on claim 25 and specifies that the method uses a decoder which includes a timer, an input to receive the transmission word, a decryption unit to decrypt the transmission word and obtain the transmitted timer information, memory to store the timer relationship value and a comparison unit to compare the transmitted timer information to time information generated by the decoder timer and to the stored timer relationship value, and means, responsive to the comparison unit, to activate an output if certain criteria are met in the comparison.

There are no timers disclosed in Farris that are equivalent to an encoder timer to influence the construction of a code word, or a constantly (with time passing) changing decoder timer.

2. REJECTION OF CLAIM 31 UNDER 35 U.S.C. 103(A)

Claim 31 is dependent on claim 30 and further specifies that a cold boot counter value, when included in the transmission word, is transmitted in the clear. Once again, the rejection is completely without merit, not only because Farris et al. do not disclose the elements of claim 25, but also because the secondary reference to Belt, U.S. Patent No. 5,446,904, fails to disclose a cold boot counter as recited in claim 31.

The cold boot counter feature of the present invention is discussed in paragraphs [0074]-[0080] on pages 16 and 17 of the specification. If an encoder suffers a temporary power failure,

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

for example, the encoder's processor must restart and go through a cold boot procedure. The cold boot counter keeps track of the number of cold boots that have occurred. This number is sent as part of the transmission word to the decoder each time the transmitter encoder is actuated by a user. If the cold boot counter is incremented, this tells the decoder that the encoder has suffered a power failure and that the encoder's timer value will therefore no longer be in synchronism with the decoder's timer value. The cold boot counter is thus a mechanism to track the number of cold boots that have occurred to maintain a high security level and overcome the loss of "real time clock" integrity without compromise to security.

The Examiner correctly observes that Farris et al. do not disclose the cold boot counter feature of the claimed invention. As an aside, this is not surprising since Farris et al. has no continuously running timers, and the effect of losing power is not a problem. In fact, it is standard practice to only activate (power) the encoder when operating the device. This helps to preserve power. Thus the concept of a cold boot counter to help maintain security when re-synchronising after a loss of power situation has absolutely no meaning in Farris et al. and not surprisingly, is not disclosed by Farris et al.

Contrary to the Examiner's assertion in the Office Action, Belt et al. fails to cure the deficiency of Farris et al. to disclose the cold boot counter function and thus cannot establish a prima facie case of obviousness under 35 U.S.C. 103. The passage in Belt et al. referred to by the Examiner, col. 38, lines 52 -- 64, refers to a procedure to recognize a "cold boot" action and activities surrounding it. This has nothing to do with a cold boot counter. There is no mention of a cold boot counter in Belt et al. and no disclosure of a mechanism to perform such count.

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

The only relevant words that can be gleaned from this passage are the words “cold boot” albeit in a totally different context. From line 55: “If it is not set, then the system is performing a cold boot and will attempt to configure itself using set-up information stored in the RAM 377 of the real time clock circuit 376.”

There is above no mention of a “cold boot counter” and no mention is made of using information concerning a real time clock circuit.

Clearly then, the Examiner’s assertion that Belt et al. disclose the feature of claim 31 is in error and provides another reason why the rejection of claim 31 should be reversed.

3. REJECTION OF CLAIMS 32, 33 AND 61-63 UNDER 35 U.S.C. 103(A)

Claims 32, 33 and 61-63 all recite various aspects of the cold boot counter feature of the claimed invention. Claim 32 recites the method of claim 25 which includes the step of keeping the encoder and decoder in synchronism using the cold boot counter which is changed each time the encoder is powered up or comes out of reset.

Claim 33 recites the method of claim 25 which includes the steps of keeping the encoder and decoder in synchronism using a cold boot counter which is changed each time the encoder is powered up or comes out of reset, and including a count value of the cold boot counter in the transmission word.

Claim 61 recites the method of claim 25, which includes the step of keeping the encoder and decoder in synchronism using a cold boot counter which is changed each time at least one of the following occurs: the encoder is powered up or comes out of reset, or loses the integrity of its timer/counter unit; and wherein the transmission word includes the encrypted data word and at

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

least a cold boot counter value that may be broken up so that several transmission words are required to transfer the complete cold boot counter value.

Claim 62 is dependent on claim 61 and specifies that the cold boot counter value, or part thereof, when included in the transmission word, is transmitted in the clear.

Claim 63 is also dependent on claim 61 and further specifies that there is a count value of the cold boot counter in the transmission word.

Once again, the Examiner relies upon a secondary reference (U.S. Patent No. 5,155,729 to Rysko et al.) in the rejection of these claims that has nothing whatsoever to do with a cold boot counter. The passage in Rysko cited by the Examiner, col. 6, lines 29 — 64, discloses a “switchover counter” which bears no similarity to a cold boot counter. This counter is used in a totally different context as evidenced by this excerpt from Col. 6, line 59: “... if the count (switch over counter value) exceeds the predetermined threshold, switchover counter 201 triggers a cold boot by...” Obviously, the counter triggers a cold boot but has nothing to do with counting the number of cold boots. Accordingly, for this reason, in addition to the reasons given in support of claim 25, the rejections of claim 32, 33 and 61-63 are also in error and should be reversed.

4. SUMMARY

Applicant has clearly demonstrated that each and every one of the Examiner’s rejections of the pending claims is completely without merit. The Examiner’s brief dismissal of Applicant’s arguments in the final Office Action in which he did not even attempt to equate specific elements in Farris et al. to each of the elements in claims 25 and 52 is unacceptable and demonstrates either a misunderstanding of the claimed invention or a misunderstanding of the

**VII ARGUMENT**  
(37 C.F.R. § 41.37(c) (1) (vii))

requirements of a reference under 35 U.S.C. 102. As has also been clearly established, many of the dependent claims recite additional features that are also not disclosed or suggested anywhere in Farris et al. Even the rejections under 35 U.S.C. 103 rely on secondary references that once again fail to disclose the elements that the Examiner concedes are not disclosed in Farris et al. Accordingly, each and every one of the claim rejections is clearly improper and should be REVERSED.

Respectfully Submitted,

By                     /wab/                      
William A. Blake  
Reg. No. 30,548

Dated: February 1, 2008  
JONES, TULLAR & COOPER, P.C.  
Customer No. 23294  
P.O. Box 2266, Eads Station  
Arlington, VA 22202  
Phone: (703) 415-1500  
Fax: (703) 415-1508  
E-mail: mail@jonestullarcooper.com

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

25. (Previously Presented) A method of securely transferring data from an encoder to a decoder, said encoder including an encoder timer and said decoder including a decoder timer, said method including the steps of:

- (a) during a learning process receiving a value of said encoder timer at said decoder and determining a mathematical difference value between said value of said encoder timer and a value of said decoder timer;
- (b) storing said mathematical difference value as a timer relationship value in said decoder;
- (c) at the encoder encrypting a data word to form a transmission word, said data word including information identifying a present value of said encoder timer;
- (d) transmitting the transmission word to the decoder;
- (e) at the decoder decrypting the transmission word; and
- (f) determining a mathematical difference value between said present encoder timer value and a present decoder timer value; and
- g) validating the transmission word by comparing the mathematical difference value between said present encoder timer value and said present decoder timer value with said timer relationship value stored in said decoder.

26. (Previously Presented) A method according to claim 25 wherein the timer relationship value in the decoder is updated upon receipt of a valid transmission word to remove any discrepancies in the relationship between the encoder timer, decoder timer and the timer relationship value, without affecting the decoder timer.



**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

27. (Previously Presented) A method according to claim 26 wherein the updating of the timer relationship value is only done when necessary.

28. (Previously Presented) A method according to claim 26 wherein the data word additionally includes at least one of the following: identity information pertaining to the encoder; command information; utility information; cold boot counter information; fixed code information; encoder power supply information and user derived information.

29. (Previously Presented) A method according to claim 28 wherein the user derived information is variable via one or more inputs to the encoder and is not known to a manufacturer of the encoder.

30. (Previously Presented) A method according to claim 25 wherein the transmission word includes the encrypted data word and at least one of the following: a cold boot counter value; command information; and identity information pertaining to the encoder.

31. (Previously Presented) A method according to claim 30 wherein the cold boot counter value, when included in the transmission word, is transmitted in the clear.

32. (Previously Presented) A method according to claim 25 which includes the step of keeping the encoder and decoder in synchronism using a cold boot counter which is changed each time the encoder is powered up or comes out of reset.

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

33. (Previously Presented) A method according to claim 25 which includes the steps of keeping the encoder and decoder in synchronism using a cold boot counter which is changed each time the encoder is powered up or comes out of reset, and including a count value of the cold boot counter in the transmission word.
34. (Previously Presented) A method according to claim 25 which includes the step of forming a plurality of transmission words, each transmission word being different from the other transmission words and being based at least on respective encoder high speed timer information, in response to a single activation of the encoder.
35. (Previously Presented) A method according to claim 25 which includes the step of forming only a single transmission word to be transmitted at least once in response to a single activation of the encoder.
36. (Previously Presented) A method according to claim 25 which includes the steps, during a learn mode, of storing learning information at the decoder which is transferred from the encoder, and deriving a key from the stored information.
37. (Previously Presented) A method according to claim 36 wherein the learning information is stored in a first-in-first-out structure.

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

39. (Previously Presented) A method according to claim 25 wherein multiple encoders are used with a single decoder comprising a single timer and multiple timer relationship values and wherein the various timer relationship values are determined, one for each encoder during its respective learning process.

40. (Previously Presented) A method according to claim 25 which includes the step of ensuring that the encoder timer at its slowest variance is faster than the decoder timer at its fastest variance.

41. (Previously Presented) A method according to claim 39 wherein, if the decoder timer lies within a predetermined window when a valid transmission word is received, the decoder timer is re-synchronized with the encoder timer by automatically adjusting the timer relationship value to remove any discrepancies in the relationship between the timers and the timer relationship value.

42. (Previously Presented) A method according to claim 41 wherein the re-synchronization is effected by a bi-directional transfer of data between the encoder and decoder.

43. (Previously Presented) A method according to claim 25 wherein the timer relationship value or a window is adjusted in size to compensate for drift between the encoder timer and the decoder timer, before validation occurs, such adjustment being

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

based at least on the time period elapsed since the last adjustment of the timer relationship value.

44. (Previously Presented) A method according to claim 25 wherein the timer relationship value or a window is adjusted in size to compensate for drift between the encoder timer and the decoder timer, such adjustment being based at least on information about the drift between the encoder timer and the decoder timer determined by analyzing at least two successive valid transmissions received with a period of time elapsed between them and said adjustment being performed before carrying out step (f) on a currently received transmission word.

45. (Previously Presented) A method according to claim 25 wherein a window size is assigned to the decoder and the encoder timer is operated to ensure that the encoder timer information does not fall outside the window for a valid transmission of a transmission word in normal operational circumstances.

46. (Previously Presented) A method according to claim 26 wherein the timer relationship value is allowed a window when validation of the transmission word occurs and the timer relationship value is adjusted based on knowledge of drift between the encoder timer, the decoder timer and the time period elapsed since a previous valid transmission of a transmission word.

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

47. (Previously Presented) A method according to claim 46 wherein the window size is dynamically adjusted and such adjustment is based on the time period elapsed since the previous adjustment of the timer relationship value.

48. (Previously Presented) A method according to claim 47 wherein the window size has a minimum value.

49. (Previously Presented) A method according to claim 47 wherein the window size has a maximum value.

50. (Previously Presented) A method according to claim 25 wherein the transmission data word also includes a timer value that changes fast so that each transmission word in a sequence of transmission words which are transmitted based on a single continuous activation of the encoder, differs from the other transmission words.

51. (Previously Presented) A method according to claim 25 wherein a higher security re-synchronization of the encoder and decoder timers is achieved at least by using the decoder to generate control signals that are used to, directly or indirectly, control the activation of the encoder.

52. (Previously Presented) Apparatus for transferring data which includes an encoder and a decoder and wherein the encoder includes a timer and an encryption unit for

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

encrypting data which includes timer information from the encoder timer, thereby to form a transmission word, and the decoder includes a decoder timer, a receiver unit for receiving the encrypted transmission word, a decryption unit for decrypting the received transmission word to extract, at least, the timer information from the encoder, a difference determination unit for determining a mathematical difference value between said encoder timer value and said decoder timer value, and a comparator unit for comparing said mathematical difference value and a timer relationship value stored in said decoder, to determine the validity of the transmission word, the timer relationship value being established during a learning process of the encoder and decoder and being representative of a mathematical difference between a value of said encoder timer that is received by said decoder during said learning process and a value of said decoder timer during said learning process.

53. (Previously Presented) Apparatus according to claim 52 which includes a unit for adjusting the timer relationship value when a valid transmission word is received to remove at least one of:

- (a) any drift that has occurred; and
- (b) any other accumulating discrepancy in the relationship between the encoder timer, decoder timer and the timer relationship value.

54. (Previously Presented) Apparatus according to claim 52 wherein the timer relationship value is adjusted before checking the validity of a received transmission

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

word, such adjustment being based at least on a known drift between the encoder timer and the decoder timer as well as the time elapsed since a previous adjustment of the timer relationship value.

55. (Previously Presented) Apparatus according to claim 52 wherein the decoder is assigned a window size which determines acceptable drift between the encoder timer and decoder timer for a valid transmission.

56. (Previously Presented) Apparatus according to claim 55 wherein the window size is adjusted before checking the validity of a received transmission word, said adjustment being based at least on the time period elapsed since the reception of a previously received valid transmission word.

57. (Previously Presented) Apparatus according to claim 52 wherein a re-synchronisation of the encoder and decoder can be achieved by the decoder providing control signals for the encoder inputs.

58. (Previously Presented) For use in the method of claim 25, a transmitter which includes an encoder timer and an encryption unit for encrypting data which at least in part is based on timer information from the encoder timer thereby to form the transmission word, and wherein the encoder timer is permitted to run only for a limited period after each activation of the transmitter.

**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

59. (Previously Presented) For use in the method of claim 25, a transmitter which includes an encoder timer and an encryption unit for encrypting data which at least in part is based on timer information from the encoder timer thereby to form the transmission word and wherein, when the encoder timer runs beyond a predetermined limit, the transmitter will upon a single activation transmit more than one transmission value equivalent to the transmitter being activated twice.

60. (Previously Presented) For use in the method of claim 25, a decoder which includes a timer, an input to receive the transmission word, a decryption unit to decrypt the transmission word and obtain the transmitted timer information, memory to store the timer relationship value and a comparison unit to compare the transmitted timer information to time information generated by the decoder timer and to the stored timer relationship value, and means, responsive to the comparison unit, to activate an output if certain criteria are met in the comparison.

61. (Previously Presented) A method according to claim 25, which includes the step of keeping the encoder and decoder in synchronism using a cold boot counter which is changed each time at least one of the following occurs: the encoder is powered up or comes out of reset, or loses the integrity of its timer/counter unit; and wherein the transmission word includes the encrypted data word and at least a cold boot counter value that may be broken up so that several transmission words are required to transfer the complete cold boot counter value.



**VIII CLAIMS APPENDIX**  
(37 C.F.R. § 41.37(c) (1) (viii))

62. (Previously Presented) A method according to claim 61 wherein the cold boot counter value, or part thereof, when included in the transmission word, is transmitted in the clear.

63. (Previously Presented) A method according to claim 61, further including a count value of the cold boot counter in the transmission word.

**IX EVIDENCE APPENDIX**  
(37 C.F.R. § 41.37(e) (1) (ix))

None

**X RELATED PROCEEDINGS APPENDIX**  
(37 C.F.R. §41.37(c) (1) (x))

None